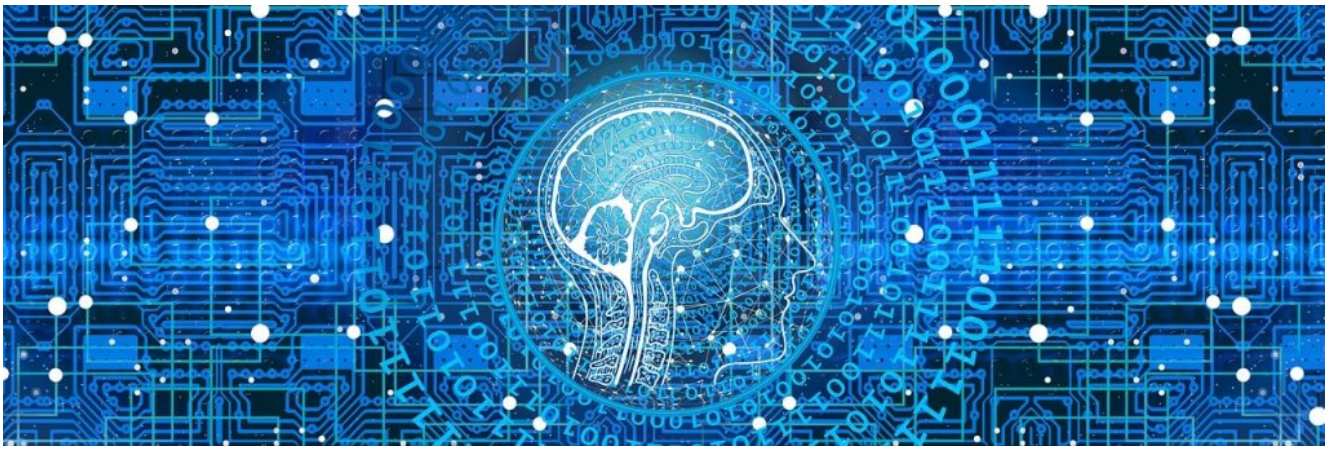
“Drones of August”: AI and the Prospects of Accidental War – Mehmet Ali Tuğtan



Artificial Intelligence and Strategic Agency

AI is permeating our lives, and the domain of security is no exception. This leads to concerns about doomsday scenarios where AI can accidentally trigger a war, or even turn against its creator, the humankind. It is natural for humans to be alarmed at the most primordial level about this latter possibility. Because humans have secured their place at the apex of the food chain not due to their superior physical qualities, but largely thanks to their frontal cortex, which gives them their freedom and agency as strategic actors -hence the unease about the replacement of human cognition, processing and decision-making with a machine counterpart. After all, it is not automation, but the autonomy of the AI that spooks us. Deep down, somewhere in our brain, genetic information passed on to us from our ancestors living on treetops in Africa is warning us about the dangerous emergence of another, faster and deadlier predator. Still, while the popular concern is centered around a kind of “Skynet syndrome”, the possibility of an accidental escalation as a result of AI to AI interaction seems to be the clearer

and more present danger. In other words, before AI becomes self aware and turns against humans, the more likely prospect for the near future is an integral accident as Paul Virilio puts it. To understand why, we first need to look at how AI works and why we keep developing it despite the risks involved.

AI in a Nutshell

Essentially, AI is a model that consist of databases and algorithms. These models can roughly be divided into 'weak' and 'strong' AI. Currently, it is the weak AI that we use through our smart devices, like ChatGPT, Siri or Alexa. Weak or narrow AI is task-specific and relies on human input to perform certain, pre-defined tasks like playing chess, self-driving cars or digital assistance. As it is, weak AI is already spooking us by anticipating our needs, responding to elaborate questions and suggesting venues of greater efficiency to direct our daily life.

Strong AI, or general AI is as yet a theoretical concept. When it comes to fruition, strong AI will have much more generalized use potential compared to weak AI, and it will possibly mimic not just human brain but human emotions as well. Strong AI will also be potentially self-aware and therefore more unpredictable compared to currently commercialized weak AI. While some experts in the field are very optimistic that strong AI will become a tangible reality within the next decade, others doubt it may ever be achieved at all.

As a rule, AI makes use of machine learning (and the somewhat mystified 'deep learning'). The main property of AI is its ability to mimic human brain functions so that tasks normally performed by humans can be delegated to AI-powered platforms, which can perform them with greater speed and accuracy. At the heart of the AI models are neural networks that enable the machine to learn a certain task on its own. But, AI also needs clean and labelled data for its datasets (the other crucial component of an AI model), and this is where things get more tricky, since in the realm of security, such data is not always easy to come by. What is more, one of the most effective ways of attacking the AI platforms of an adversary is to 'poison' their databases. Thus, protection of the AI itself increasingly

becomes an issue.

Uses of AI in Defense and Security

Currently, AI is deployed in several offensive and defensive roles including cybersecurity, surveillance and reconnaissance, trend analysis, threat detection and training simulations. Counter-missile or -drone systems like the Israeli missile defence system, Iron Dome also make use of AI. Like Strong AI, the real potential of AI in defense and security is also yet to be realized.

In the near future, we will increasingly see AI onboard autonomous offensive systems like unmanned armed land, sea and aerial vehicles. The idea of 'killer robots', or the removal of human decision from the act of killing has raised a lot of ethical and legal issues, but several armed forces around the world are already deploying lethal autonomous weapons systems (LAWS). Because at the end of the day, LAWS prove much more cost-efficient and protect the lives of soldiers. Thus, both economically and politically, it is very difficult to resist the temptation to replace humans with robots in combat environments, since when they are hit by enemy fire, robots do not return home in body bags or receive veterans benefits for the rest of their lives. What is more, once produced and deployed in scale, LAWS cost a fraction of training and maintaining human soldiers in the same role.

In the near future, AI will also be increasingly used not just to detect but to predict threat. The scope, speed and accuracy of these systems will be so great, that removing humans from the chain will be necessary to benefit from their full potential, since human intervention will only slow things down. For example, at some point it is conceivable that there will be an ongoing cyber war between opposing AI platforms so fast that human intervention is impossible without risking potential defeat. At the cybersecurity realm, defeat means collapse of critical infrastructure and irreparable damage to economy.

Even more frightening is the prospect of the integration of AI threat prediction to

AI controlled LAWS, which would practically make AI capable of starting a war without human intervention. But again, to benefit fully from the speed and accuracy of these systems, removing humans from the chain will become more and more tempting an option. This may lead to a chain reaction that will resemble the 'Guns of August' syndrome that led up to the First World War where the politicians and diplomats could not intervene in the chain reaction created by pre-conceived mobilization plans and consequent military action.

In our case, it will be conceivable for 'our AI' to launch armed drones to pre-empt a predicted threat from an adversary, who also relies on an AI system to monitor our threat to them. Thus, 'their AI' will simultaneously defend and counter-attack using a variety of tools ranging from cyber-offensive capabilities to LAWS on stand-by. As this process unfolds almost at lightning speed, human politicians, diplomats and military leaders will be too slow to understand, let alone intervene in, what's going on between the 'Drones of August' of both sides.

Before sounding the alarm, however, we must also stress that these predictions are neither inevitable nor self-fulfilling: on the contrary, just as these trends become clearer, there is a growing move towards more regulated use of AI in the realm of security and defense. Most recently, the Biden Presidency has issued an Executive Order to protect American citizens from the growing risks of AI. At the end of the day, these systems will rely on algorithms written by humans (At least initially) and datasets compiled by humans (Again, at least initially). Most importantly, it will be our decision to integrate threat prediction systems with LAWS. Thus, in conclusion we can say that there is still "No fate but what we make".

Dr. Mehmet Ali Tuğtan, İstanbul
Bilgi University

Dr.
Faculty Member Mehmet Ali Tuğtan has been a faculty member at the Department of
International Relations at Istanbul Bilgi University since 2008. He received his PhD degree from Boğaziçi University Political Science program in 2008. His

areas of expertise are Turkish-American Relations, Current World Policy and Security Studies.

To cite this work: Mehmet Ali Tuğtan, ""Drones of August": AI and the Prospects of Accidental War", Panorama, Online, 8 December 2023, https://www.uikpanorama.com/blog/2022/12/23/mat/
